23-811 C

Case No: _____

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

Larry Golden
Plaintiff, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net
(864) 992-7104

LARRY GOLDEN,

Plaintiff,

V.

THE UNITED STATES DEFENSE THREAT REDUCTION AGENCY

Defendant.

Patent Infringement Pursuant to 28 U.S.C. Section 1498

May 29, 2023

INFORMAL COMPLAINT

1. Under the Tucker Act, the United States Court of Federal Claims has jurisdiction to adjudicate a claim if the statute, regulation, or constitutional provision that is the basis for that claim "can fairly be interpreted as mandating compensation by the Federal Government for the damage sustained," *United States v. Mitchell*, 463 U.S. 206, 217 (1983), and the plaintiff is "within the class of plaintiffs entitled to recover under the statute if the elements of [the] cause of action are established," *Greenlee County, Arizona v. United States*, 487 F.3d 871, 876 (Fed. Cir.

2007). "There is no further jurisdictional requirement that plaintiff make [] additional nonfrivolous allegation[s] that [he] is entitled to relief under the relevant money-mandating source." *Jan's Helicopter Serv., Inc. v. Federal Aviation Agency*. 525 F.3d 1299, 1307 (Fed. Cir. 2008)."

2. This is a claim pursuant to 28 U.S.C. § 1498(a) for recovery of Plaintiff's reasonable royalties for the unlicensed use, manufacture for, or by the United States, inventions described in and covered by United States Patent Numbers: 9,096,189; 9,589,439, and 10,163,287. **Exhibits A, B, & C**

JURISDICTION

3. The jurisdiction of this Court is based on the provisions of 28 U.S.C. § 1498(a).

4. 28 U.S.C. § 1498(a): Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture.

THE PARTIES

5. Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business (ATPG Technology, LLC), and residence at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

6. Defendant, the UNITED STATES DEFENSE THREAT REDUCTION AGENCY (DTRA). The DTRA is both a defense agency and a combat support agency within the U. S. Department of Defense (DoD) for countering weapons of mass destruction and supporting the nuclear enterprise. DTRA provides cross-cutting solutions to enable the DoD, the United States Government, and international partners to deter strategic attack against the United States and its allies; prevent, reduce, and counter WMD and emerging threats; and prevail against WMD-armed adversaries in crisis and conflict. The Solicitation for this initiative is attached as **Exhibit D: DTRA HDTRA-19-S-0005 BAA Call CBI-01**

STANDARD(S) FOR REVIEW

7. When the United States Court of Appeals for the Federal Circuit in Plaintiff's cases *Golden v. Apple Inc. et al* Case No. 22-1229 and *Golden v. Google* Case No. 22-1267, before filing an opinion on 09/08/2022, the three Circuit Judges of Dyk, Taranto, and Stoll used as their standard of review the following:

> "Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. This standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted). In the patent context, this court has explained that a plaintiff need not "plead facts establishing that each element of an asserted claim is met," *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged." *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556). We review the district court's dismissal of the complaint *de novo*. *Anand v. Ocwen Loan Servicing, LLC*, 754 F.3d 195, 198 (4th Cir. 2014)."

8. Upon review, the three Circuit Judges of Dyk, Taranto, and Stoll considered ***all*** of the previous cases directly related to the Apple and Google cases [case nos. 22-1229 and 22-1267] that was currently before the Circuit Court; and, the recommendations, decisions, opinions, and judgements.

9. The Circuit Judges decided not to dismiss Plaintiff's cases based on the number of times Plaintiff was forced to file because of Court errors [changing the cause of action; improperly petitioning the PTAB; giving the Government another chance at dismissing Plaintiff's case; making a Section 1491(a) the same as a Section 1498(a); CFC adjudicating a 35 U.S.C. Section 271(a) which is outside the Court's jurisdiction; making a violation of antitrust laws the same as 35 U.S.C. Section 271(a); wrongfully dismissing as duplicative; wrongfully

dismissing because of page count, etc.] The *Golden v. Apple* case was dismissed ***without prejudice*** for the following reason:

> "Mr. Golden does not argue that the docketed complaint contains factual allegations beyond those contained in his original complaint or that the allegations in the docketed complaint do anything beyond listing the alleged infringed-upon patent claims and the alleged infringing devices. This is plainly insufficient. We see no error in the district court ***without prejudice*** dismissal of the Apple case."

10. In *Golden v. Google* CAFC Case No. 22-1267, the case was Vacated and Remanded back to the District Court for the following reason: **Exhibit E**

> "In the Google case, the district court again concluded that Mr. Golden's complaint was frivolous. Here, however, Mr. Golden's complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189. The district court discounted this claim chart because it "contains the exact same language as the claim charts previously rejected by the Federal Circuit [in the 2019 case], although Google Pixel 5 Smartphone appears in the far-left column instead of Apple." Dist. Ct. Op. at 4. But to the extent that the chart includes the "exact same language" as previously rejected charts, it is simply the language of the independent claims being mapped to. The key column describing the infringing nature of the accused products is not the same as the complaint held frivolous in the 2019 case. It attempts—whether successfully or not—to map claim limitations to infringing product features, and it does so in a relatively straightforward manner. We conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart. On remand, the district court should allow the complaint to be filed and request service of process [] … We express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous."

11. The Defendants in both cases asked the three Circuit Judges of Dyk, Taranto, and Stoll to affirm dismissal of Plaintiff's cases because the cases are "frivolous" and that Plaintiff is a "serial filer". The Circuit Judges reviewed the District Court case and decided against it.

12. What that means is, the Defendant (Government the United States) is collateral estoppel from re-litigating the issue of "frivolousness"; the number of times Plaintiff has file cases; and the cause of actions of those cases, because the issues were actually litigated and conclusively resolved by the three Circuit Judges of Dyk, Taranto, and Stoll in *Golden v. Google* CAFC Case No. 22-1267.

13. Issue preclusion, or collateral estoppel, precludes a party [Government] from relitigating an issue actually decided in a prior case and necessary to the judgment. In a collateral estoppel case, the issue at the heart of the claim has already been raised and litigated in *Golden v. Google* CAFC Case No. 22-1267.

14. According to law, any and all defense pleadings of "frivolousness" the Government presents in this case to prejudice Plaintiff, after the *OPINION* filed on 09/08/2022 in *Golden v. Google* Case No. 22-1267, should be disregarded and stricken because of "issue preclusion" and "collateral estoppel".

NATURE OF THE CASE

15. Plaintiff included in this complaint a claim chart that is practically identical to the Google complaint and claim chart. Stare decisis is the legal doctrine Plaintiff is relying on because it obligates this Court to follow historical cases when making a ruling on a similar case.

16. Stare decisis ensures Plaintiff that cases with similar scenarios and facts are approached in the same way. Simply put, it binds this Court to follow the legal precedent set by the Federal Circuit in its previous decision in Golden v. *Google* CAFC Case No. 22-1267.

17. To demonstrate this is not an incidental occurrence Plaintiff provided this Court with a smartphone comparison chart of the Google Pixel 5; Apple iPhone 12; Samsung Galaxy S21; LG V60 ThinQ 5G; & Asus/Qualcomm Smartphone for Snapdragon Insiders. The results are the same, they all have virtually identical elements in their alleged infringing products.

18. Plaintiff has cured the deficiencies identified in *Golden v. US* CFC Case No. 13-307C. Plaintiff responded to the deficiencies only because this Court allowed the Government to present a defense whereby the sensors had to by "native" to the alleged infringing products. The Federal Circuit disagreed in *Golden v. Google* CAFC Case No. 22-1267 and determine the detection capability can also be CBRN plugins. Third party contractors cannot be held liable for

infringement if performing work for the Government, and with the Government's authorization and consent.

19. Plaintiff has reproduced a claim chart in this complaint that illustrates sensing mechanisms "native" to the smartphones manufactured by Google, Apple, Samsung, LG, and Qualcomm. The sensing mechanisms include the smartphone cameras, standard sensors, and ports.

20. To support Plaintiff's claim of products (communication devices) grouped together by common features of design similarities of at least that of a smartphone, a PC, etc. Plaintiff added to the smartphone group a Hewlett Packard PC to demonstrate infringement.

VIOLATION ALLEGED

The United States Department of Defense, "Defense Threat Reduction Agency (DTRA)" has Authorized and Consented to the Infringement of Plaintiff's Patents.

21. Upon information and belief, the United States Defense Threat Reduction Agency (DTRA), (the United States), beginning in year 2019, with the initiative DTRA HDTRA-19-S-0005 BAA Call CBI-01 has allegedly infringed claim 5 of Plaintiff's '287 patent, claim 23 of Plaintiff's '439 patent, and claim 1 of Plaintiff's '189 patent. Pursuant to the guidelines of 28 U.S.C. § 1498(a): "[w]henever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture", Plaintiff believes the DTRA has "authorized or consented" to the infringement of Plaintiff's '287, '439, and '189 patents.

22. As a result of implied authorization or consent; the DTRA required the contractors of Draper, Microsoft, Intel, Hewlett Packard, Google, Apple, Samsung, LG, and Qualcomm to integrate "for the Government" its, hazard-awareness-and-response tools into the ATAK, iTAK, and WinTAK for chemical and biological agents and radiological and nuclear threats (CBRN) detection and reporting. Further, the contractors integrated, assembled, modified, or developed CBRN plugins for an end-user device such as Plaintiff's patented smartphones, PCs, and tablets.

AUTHORIZATION OR CONSENT

23. The Research & Development Directorate, Chemical and Biological (RD-CB) Department of the Defense Threat Reduction Agency (DTRA) issued on May 7, 2019, a Broad Agency Announcement (BAA) Call CBI-01 "Chemical and Biological Threats: Tactical Assault Kit (TAK) Plugins for Warning & Reporting and Decision Making" under BAA HDTRA1-19-S-0005.

24. Under the implied authorization or consent, Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard have "manufactured for the Government" products and devices that allegedly infringes claim 5 of Golden's '287 patent, claim 23 of Golden's '439 patent, and claim 1 of Golden's '189 patent.

25. The government's authorization of or consent to a contractor's infringing activity may be express or implied, *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976). To succeed on an implied authorization theory there must be some explicit government action, such as a contracting officer's instruction, or evidence extrinsic to the contract language showing the government's intention to assume liability, *Va. Panel*, 133 F.3d at 870; *Larson*, 26 Cl. Ct. at 370.

26. In *Larson v. United States*, the Claims Court recognized that implied authorization "may be found under the following conditions: (1) the government expressly contracted for work to meet certain specifications; (2) the specifications cannot be met without infringing on a patent; and (3) the government had some knowledge of the infringement." *Larson*, 26 Cl. Ct. at 370 (citing *Bereslavsky v. Esso Standard Oil Co.*, 175 F.2d 148, 150 (4th Cir. 1949); *Carrier Corp. v. United States*, 534 F.2d 244, 247–50 (Ct. Cl. 1976); *Hughes*, 534 F.2d at 897–901).

27. The purpose behind permitting the government's authorization or consent to be implied is tied to the government's need to procure items without disruption, *TVI Energy*, 806 F.2d at 1060; *Robishaw Eng'g Inc. v. United States*, 891 F. Supp. 1134, 1145 (E.D. Va. 1995) ("[T]he policy purpose behind § 1498 is to insulate the government and its private contractors from 'lawsuits disruptive of the procurement process.'" (quoting H.R. Rep. No. 872, 82d Cong., 1st Sess. 1420 (1951), as it appears in *Northrop Corp. v. McDonnell Douglas Corp.*, 705 F.2d 1030, 1041 (9th Cir. 1983))), and avoid the need for government agencies to perform an exhaustive patent search for products or services they wish to procure.

28. For example, in *TVI Energy*, the Federal Circuit found implied authorization or consent where the government required a contractor to demonstrate an allegedly infringing device as part of bidding requirements under a United States military solicitation for disposable thermal targets, 806 F.2d at 1060–61. Following the demonstration, one bidder/patent owner, TVI Energy, sued a competing bidder, Blane, for patent infringement. Blane asserted immunity under § 1498(a), despite having no express letter of consent or authorization from the government to infringe any patent. The Federal Circuit nevertheless found implied authorization, stating that "[t]o limit the scope of § 1498 only to instances where the Government requires by specification that a supplier infringe another's patent would defeat the Congressional intent to allow the Government to procure whatever it wished regardless of possible patent infringement."

29. Courts have often found a contractor, through the government's implied authorization, to be immune from suit from the time it offers to supply or begin to manufacture products for the government, See, e.g., *Robishaw*, 891 F. Supp. at 1141 (citing *Trojan, Inc. v. Shat-R-Shield, Inc.*, 885 F.2d 854, 856–57 (Fed. Cir. 1989); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1282–83 (Fed. Cir. 1988); *TVI Energy*, 806 F.2d at 1059–60; *Stelma, Inc. v. Bridge Elecs.* Co., 287 F.2d 163, 164 (3d Cir. 1961)).

30. If these two elements—acting "for the government" with its "authorization or consent"—are met, then a contractor who infringes a patent in the course of its performance of work for the government, under any definition of infringement in § 271 of the Patent Act, is shielded from liability. In this respect, § 1498(a) serves as an affirmative defense available to government contractors in patent infringement actions in district court, *Advanced Software Design Corp. v. Fed. Reserve Bank of St. Louis*, 583 F.3d 1371, 1375 (Fed. Cir. 2009); *Toxgon Corp. v. BNFL, Inc.*, 312 F.3d 1379, 1381–82 (Fed. Cir. 2002).

31. Correlatively, where the government has assumed a contractor's liability, a patent owner can seek judicial relief by filing suit against the government in the USCFC, *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359, 1363 (Fed. Cir. 2014). However, various government agencies have internal processes to hear administrative claims for patent infringement. Christine Hlavka, Contractor Patent Bandits: Preventing the Government from Avoiding 28 U.S.C. § 1498 Liability for Its Contractors' Unauthorized Use of Patented Material by Outsourcing One or More Steps of the Process Abroad, 37 Pub. Cont. L.J. 321, 324–25 (2008).

32. Therefore, for Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard "authorization or consent of the Government," does not need to be expressly stated. *See TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986) ("[a]uthorizarion or consent by the Government can be express [or] [i]n proper circumstances, Government authorization can be implied."). Indeed, "authorization or consent . . . may be given in many ways other than by . . . direct form of communication--e.g., by contracting officer instructions, [or] by specifications . . . which impliedly sanction and necessitate infringement[.]" *Hughes Aircraft co*, 534 F.2d at 901.

33. In light of the allegations that the inventions disclosed in patents '287, '439 and '189 were designed to prevent terrorist activity, it is plausible that Draper, Microsoft, Google, Apple, Samsung, LG, Qualcomm, Intel, and Hewlett Packard manufactured infringing devices for the benefit of DTRA to promote national security' see, e.g., *Hughes Aircraft Co.*,534 F.2d at 898 (finding that the government's participation in a satellite program was "for the Government," because the program was vital to the military defense and security of the United States). Moreover, under section 1498(a), "Government authorization or consent" can be implied by circumstances. *See TVI Energy Corp.* 806 F.2d at 1060'

34. DTRA Government funding of research that led to the development and testing of the accused devices (e.g., CBNE Plugins; applications; chips) supports a reasonable inference that the Government impliedly sanctioned the infringing activity.

35. A review of the claim charts presented in this Complaint against the Defense Threat Reduction Agency (DTRA) identifies by name; by name and product number; or by name, model and product number, the devices that allegedly infringes Plaintiff's patents.

ANDROID TEAM AWARENESS KIT (ATAK)

36. Android Team Awareness Kit (ATAK) is an Android smartphone geospatial infrastructure and military situation awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing.

37. Android is a mobile operating system based on a modified version of the Linux kernel and other open-source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. Android is developed by a consortium of developers known as

the Open Handset Alliance, though its most widely used version is primarily developed by Google. It was unveiled in November 2007, with the first commercial Android device, the HTC Dream, being launched in September 2008.

38. At its core, the operating system is known as Android Open-Source Project (AOSP) and is free and open-source software (FOSS) primarily licensed under the Apache License. Over 70 percent of smartphones based on Android Open-Source Project run Google's ecosystem (which is known simply as Android)

39. Android has been the best-selling OS worldwide on smartphones since 2011 and on tablets since 2013. As of May 2021, it had over three billion monthly active users, the largest installed base of any operating system

40. This Android app is a part of the larger TAK family of products. ATAK has a plugin architecture which allows developers to add functionality. This extensible plugin architecture that allows enhanced capabilities for specific mission sets (Direct Action, Combat Advising, Law Enforcement, Protection Operations, Border Security, Disaster Response, Off-grid Communications, Precision Mapping and Geotagging).

41. ATAK was initially created in 2010 by the Air Force Research Laboratory, and based on the NASA WorldWind Mobile codebase its development and deployment grew slowly, then rapidly since 2016. The Android Team Awareness Kit or TAK is currently used by thousands of Department of Homeland Security personnel, along with other members of the Homeland Security Enterprise including state and local public safety personnel. It is in various stages of transition across DHS components and is the emerging DHS-wide solution for tactical awareness.

42. In addition to the Android version, there is also a Microsoft Windows version (WinTAK), an Apple iOS version (iTAK), and finally a Virginia-based military tech firm's (LucyTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with to provide similar functionality on a Windows platform.

43. In January 2015, AFRL began licensing ATAK through TechLink to U.S. companies, for commercial use to support state/local government uses as well as civilian uses. As of January 2020, one hundred companies have licensed ATAK for commercial uses. As of

March 31, 2020, the civilian version of ATAK, referred to as CivTAK has been approved for "Public Release" by Army Night Vision and is available for download on takmaps.com And subsequently named Android Team Awareness Kit (ATAK) - Civilian.

44. The Defense Threat Reduction Agency (DTRA) has leveraged TAK for enhanced CBRNE situational awareness with the goal of protecting military and civilian populations from intentional or incidental chemical or biological threats and Toxic Industrial Chemicals/Materials (TIC/TIM) hazards.

45. Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

46. Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK). ATAK is a digital application available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. Warfighters use ATAK to guide themselves to safety when confronted with a release of chemical and biological agents and radiological and nuclear threats (CBRN).

47. ATAK can connect to sensors on many platforms (e.g., satellites, drones, smartwatches) and has many plugins that warfighters can download. ATAK provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.

48. Warfighters positively evaluated the CBRN plug-ins at the 2019 Chemical and Biological Operational Analysis (CBOA) event, where warfighters evaluated several technology prototypes for their utility in chemical and biological defense. Warfighters reported that the CBRN capabilities in ATAK are useful and easy to use with minimal training.

49. Overall, the U.S. armed forces and their interagency and coalition partners value ATAK and the common operating picture it provides. DTRA continues to develop CBRN-specific plug-in capabilities to support warfighters on the battlefield.

SMARTPHONE COMPARISON BETWEEN THE GOOGLE PIXEL 5; APPLE iPHONE 12; SAMSUNG GALAXY S21; LG V60 ThinQ 5G; & ASUS / QUALCOMM SMARTPHONE FOR SNAPDRAGON INSIDERS

50. The Federal Circuit on 09/08/2022, in *Larry Golden v. Google LLC*; Case No. 22-1267 — "VACATED AND REMANDED" the relevant Case No: 22-1267 Document 15; back to the District Court "to be filed and request service of process".

51. The Federal Circuit determined the complaint, "includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189" … "in a relatively straightforward manner" … and that the [Circuit] "express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous." **Exhibit E**

> Three-Judge Panel: "DISCUSSION. 'Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal,* 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege "enough facts to state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570 … [T]his standard "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted) … this court has explained that a plaintiff … must plead "'enough fact[s] to raise a reasonable expectation that discovery will reveal' that the defendant is liable for the misconduct alleged."
>
> "Mr. Golden's complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 … It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner …[W]e conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart.…"

Claim Chart for the Google Pixel 5 Smartphone (Federal Circuit)

The following Claim Chart is an illustration of literal infringement. At least one of the alleged infringing products of Google (i.e., Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), or 5) is representative of most all the above alleged infringing products of Google asserted in this complaint. At least one of the alleged infringing products of Google (Google Pixel 5) is illustrated to show how the Google Pixel 5 allegedly infringes on at least one of the asserted independent claims of each of the patents-in-suit ('287, '439, and '189 patents).

Google Pixel 5 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
	A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;

Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X
Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	at least one motion sensor in communication with the at least one CPU;	X	X
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of… WiFi connection, internet connection, radio frequency (RF) connection, cellular connection… capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group… of satellite, Bluetooth, WiFi…
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a… Bluetooth connection, WiFi connection, internet connection… cellular connection… short range radio frequency (RF) connection, or GPS connection;	X
Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;	whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;	X

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X
BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use
Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween…

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;	wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU…	X	X
Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or… detect at least one of a chemical biological… agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device; a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;

Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	X	X	whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	X	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection… short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X

I. Central Processing Units (i.e., CPUs, Processors, Chipsets, SoC)

1. Android Platform (i.e., Android Operating System (OS))

a. Application Specific for CBRNE Detection

i. Communication Protocol (i.e., Plug-ins, Bluetooth, Cellular, NFC)

The smartphone has come a long way since the first iPhone launched in 2007. While Apple's iOS is arguably the world's first smartphone operating system, Google's Android is by far the most popular. Android has evolved significantly since first being released on an HTC-made T-Mobile device in 2008.

It wasn't until 2005 that Google purchased Android, Inc., and while there wasn't much info about Android at the time, many took it as a signal that Google would use the platform to enter the phone business. Eventually, Google did enter the smartphone business — but not as a hardware manufacturer. Instead, it marketed Android to other manufacturers, first catching the eye of HTC, which used the platform for the first Android phone, the HTC Dream, in 2008.

List of Features Supported by Google Android Tactical Assault Kit, (ATAK) (or the Android Team Awareness Kit, (ATAK))

- **BIOMETRICS**: Biometric factors allow for secure authentication on the ***Android platform***. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).

- **DISABLING LOCK MECHANISM:** ***Google's Android operating system*** features a lock mechanism to secure your phone, known as pattern lock. When setting the pattern, you must drag your finger along lines on the screen between different nodes. Afterward, to unlock the phone, you'll need to replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. If you can't log in, you'll have to employ some other methods to restore control of your phone.

- **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) DETECTION:** Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the *Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK)*. ATAK is a digital application available to warfighters throughout the DoD. Built on the ***Android operating system***, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

- **HEART RATE**: *Android Team Awareness Kit, ATAK* provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.

- **NEAR FIELD COMMUNICATION (NFC)**: Pixel™, Phone by Google - Turn NFC on/off. ***Near Field Communication (NFC)*** allows the transfer of data between devices that are a few centimeters apart, typically back-to-back. NFC must be turned on for NFC-based apps (e.g., Tap to Pay) to function correctly. NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity.

- **WARFIGHTERS:** The U.S. armed forces and their interagency and coalition partners value *Android Team Awareness Kit, ATAK* and the common operating picture it provides. DTRA continues to develop ***CBRN-specific plug-in capabilities*** to support warfighters on the battlefield.

The Alleged Infringing Smartphones Google, Apple, Samsung, LG, and Qualcomm that Support either the ATAK or the iTAK

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
				
Chipset: Qualcomm Snapdragon 765G **CPU**: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) **OS**: Google Android 11, upgradable to Android 13. **Modem**: Snapdragon® X52 5G Modem-RF System.	**Chipset:** Apple A14 Bionic (5 nm). **CPU**: Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm). **OS**: iOS 14.1, upgradable to iOS 16.1 **Modem:** Qualcomm's Snapdragon X55 5G modem	**Chipset:** Qualcomm SM8350 Snapdragon 888 5G (5 nm). **CPU:** Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55) - USA/China. **OS**: Google Android 11, upgradable to Android 13 **Modem**: Snapdragon® X60 5G Modem-RF System.	**Chipset**: Qualcomm SM8250 Snapdragon 865 5G (7 nm+). **CPU:** Octa-core (1x2.84 GHz Cortex-A77 & 3x2.42 GHz Cortex-A77 & 4x1.80 GHz Cortex-A55). **OS**: Google Android 10, upgradable to Android 13 **Modem:** Qualcomm's Snapdragon X55 5G modem	**Chipset:** Qualcomm SM8350 Snapdragon 888 5G (5 nm) **CPU:** Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55). **OS**: Google Android 11. **Modem**: Snapdragon® X60 5G Modem-RF System.
Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Temperature sensors located within; the sensors monitor the battery and processor's temperature. In extreme temperatures (hot or cold), these sensors shut down the device to prevent damage	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Accelerometer (gravity sensor) supported by the iOS platform. Accelerometer/ Motion sensor: This sensor helps the screen automatically switch from landscape to portrait modes and back again based on whether you're holding the phone vertically or horizontally.	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	Adjusts the screen brightness for current light conditions using the built-in ambient light sensor. Screen: 6.1" Super Retina XDR (OLED). Lock the screen orientation so that it doesn't change when the iPhone is rotated.	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.2 inches flexible OLED display at 421 ppi	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.8 inches, 109.8 cm2 OLED display at 395 ppi density	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.78 inches, 109.5 cm^2 OLED display at 395 ppi density
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Apple's iOS operating system features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable). Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.	Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	USB-A to Lightning cable or the newer USB-C to Lightning cable with your iPhone. The MagSafe Battery Pack makes on-the-go, wireless charging easy and reliable—just attach it to your iPhone	Samsung USB-C Cable lets you charge your USB-C device as well as sync your data to your smartphone	UrbanX USB-C to USB 3.1 Adapter, USB-C Male to USB-A Female, Uses USB OTG Technology, Compatible with LG V60 ThinQ 5G	ASUS / Qualcomm Smartphone for Snapdragon Insiders Dual Port 32GB USB Type C Memory Stick; 32GB USB Type-C flash drive; Features USB Type-C connector and a traditional USB connector.
BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	Apple's iOS operating system allows for Face ID authentication with the iPhone 12. The phone also features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable). Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID, Touch ID, or enter a passcode.	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).

Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)
Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID, or enter a passcode. *iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies

Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID-Touch ID or enter a passcode. *iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies	Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone. *Android Team Awareness Kit*, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies
Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*iOS Team Awareness Kit*, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.	*Android Team Awareness Kit*, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.

Figure 1

Google's "use" of Plaintiff's Patented Central Processing Units (CPUs)

"[T]he Accused Products (i.e., Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones) , which are "computers" (i.e., cell phones, computer tablets, and laptops), include components of a memory, a display, and a ***processor***" … "[w]hen in use, the "Find My Device" pre-loaded onto the Accused Product uses a ***processor***" … "[t]he "Find My Device" feature displays [] information through a ***processor*** using data stored in the device's memory" … "[t]he LG Support Page lays out in a step-by-step process how to correctly remotely log in to the ***processor*** to access [] lock the device" … *See Carolyn Hafeman v. LG Electronics Inc.*

In the above claim chart, the Google, Samsung, LG, and Asus/Qualcomm smartphones have Qualcomm Snapdragon Chipsets; have Octa-core CPUs (***processors***); have Google Android Operating Systems; have Qualcomm Snapdragon Modems; have Google "Find My Device" pre-installed *See Carolyn Hafeman v. LG Electronics Inc.*; have Google Android Team Awareness Kits; have Megapixel cameras for CBR sensing; have cameras for captioning nanopores; Biosensors for CBRNE detection; and, Plug-Ins for CBRN detection.

Figure 2 is a comparative chart of the "megapixel" smartphone cameras used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK or iTAK.

Google Pixel 5 Smartphone	**Apple iPhone 12 Smartphone**	**Samsung Galaxy S21 Smartphone**	**LG V60 ThinQ 5G**	**Asus / Qualcomm Smartphone for Snapdragon Insiders**
Google Pixel 5: Dual - 12.2 MP (megapixel), OIS 16 MP (megapixel) Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A ***megapixel*** camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the ***pixel*** resolution phone camera. ***Megapixel*** resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	***Apple iPhone 12: Dual - 12 MP (megapixel), OIS 12 MP (megapixel)*** Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A *megapixel* camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the *pixel* resolution phone camera. *Megapixel* resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	***Samsung Galaxy S21: Triple - 12 MP (megapixel), OIS 64 MP (megapixel)*** Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A ***megapixel*** camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the ***pixel*** resolution phone camera. ***Megapixel*** resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	***LG V60 ThinQ 5G: Dual - 64 MP (megapixel), OIS 13 MP (megapixel)*** Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A ***megapixel*** camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the ***pixel*** resolution phone camera. ***Megapixel*** resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html	***Asus / Qualcomm: Triple - 64 MP (megapixel) OIS; 8 MP, 12MP (mega)*** Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A ***megapixel*** camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the ***pixel*** resolution phone camera. ***Megapixel*** resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: https://www.understandingnano.com/cell-phone-sensors-toxins.html

Figure 2

Figure 3 is a visual display of different ways the smartphone camera [1] [2] can be used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK or iTAK.

Figure 3

---

1 The camera captures the image from the array of nanopores that uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the resolution phone camera. The resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time*. Source: https:// www.understanding nano.com/cell-phone-sensors-toxins.html

2 Hyperspectral imaging scans for light frequencies that humans can't see in order to identify the unique chemical signatures of different substances. They say their device, which can be mass produced, is compatible with all standard smartphone cameras. *These New Smartphone Cameras Could Tell You What an Object Is Made of* https://www.sciencealert.com/new-smartphone-cameras-could-tell-you-what-an-object-is-made-of

Figure 4 describes how at least nine (9) standard sensors for the Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones can be used as "biosensors". Each Biosensor qualifies as an alternative to ATAK or iTAK.

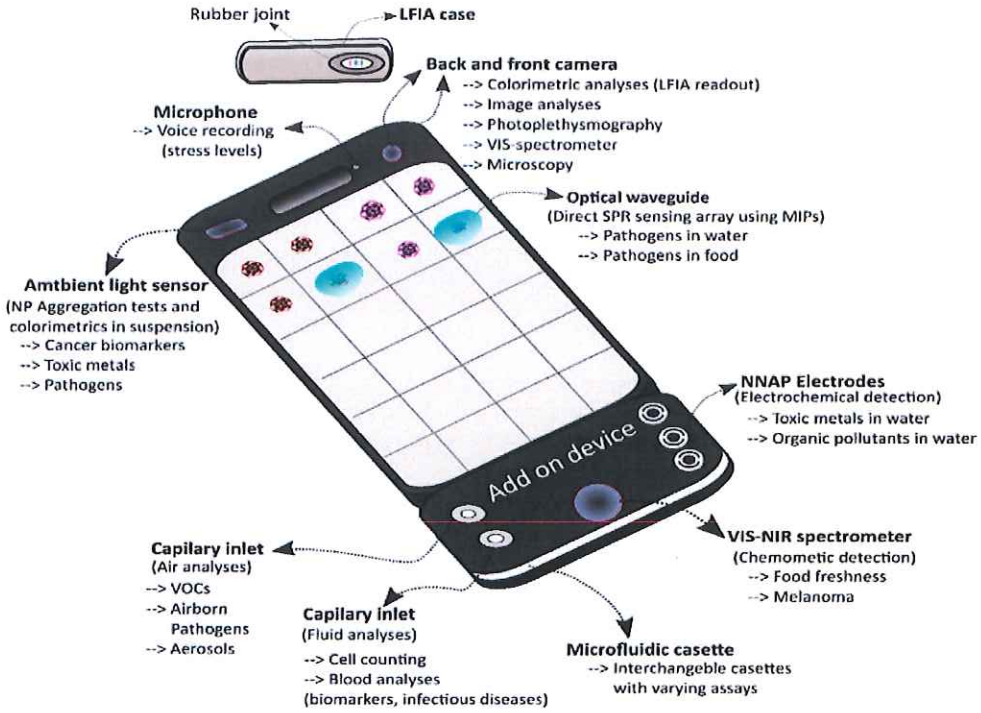

Figure 4

The Smartphones Biosensors:

1. Ambient light sensor: Cancer biomarkers; Toxic metals; Pathogens
2. Capillary inlet: (Air analysis). Airborne Pathogens; Aerosols
3. Capillary inlet: (Fluid analysis). Blood analysis; Biomarkers
4. Microfluidic cassette: Interchangeable cassettes with varying assays
5. VIS-NIR spectrometer: Food freshness; Melanoma
6. NNAP Electrodes: Toxic metals and Organic pollutants in water
7. Optical Waveguide: Pathogens in water and food
8. Back and front camera: Colorimetric analysis; Image analysis
9. Microphone: Voice recording stress levels

Figure 5 list some of the same standard sensors illustrated in Figure 4. The port on smartphones is used for the CBRN ***plug-ins*** included in ATAK or iTAK.

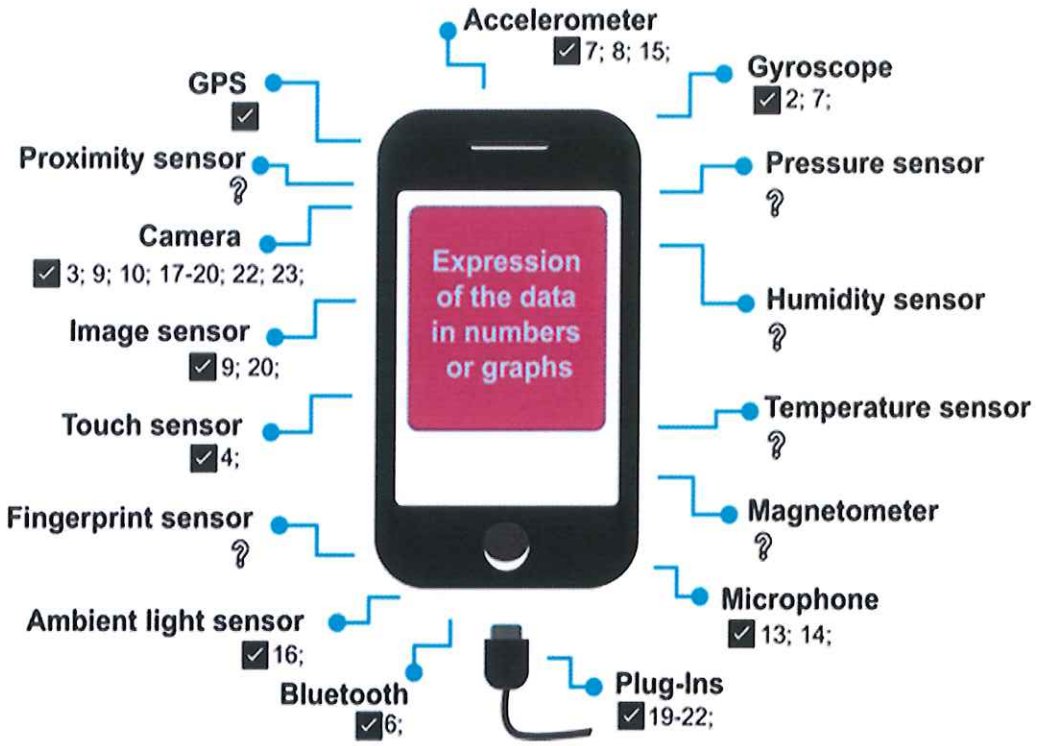

Figure 5

ATAK and iTAK are digital applications available to warfighters throughout the DoD. Built on the Android operating system and iOS operating systems, ATAK and iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK and iTAK now includes chemical, biological, radiological, and nuclear (CBRN) ***plug-ins***.

Just having a plug-in is not all that's involved. There has to be an app specific software to sync the chemical, biological, radiological, and nuclear sensors to the smartphone plus the Google Android Operating System.

MICROSOFT WINDOWS (WINTAK)

52. In addition to the Android version (ATAK) CBRN plug-ins for smartphones, there is also a Microsoft Windows version (WinTAK). WinTAK is an application developed for the Microsoft Windows Operating System which uses maps to allow for precise targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. It was developed in conjunction with ATAK to provide similar functionality on a Windows platform.

53. The Defense Innovation Marketplace is your centralized source for Department of Defense (DoD) science and technology (S&T) planning, acquisition resources, funding and financial information. Under the Broad Agency Announcement from the Joint Science and Technology Office (JSTO) Digital Battlespace Management Division, DTRA funded the development of ATAK, WinTAK, and WebTAK compatible versions of existing decision support tools for chemical and biological warning and reporting, hazard prediction, and consequence assessment.

54. ATAK is an Android®-based GIS moving map application. WinTAK is Microsoft Windows®-based. ATAK was developed to provide SpyGlass-like C2, Situational Awareness and planning capabilities on smartphones and tablets. WinTAK was developed to provide a Windows-based application with a user interface similar to ATAK.

55. ATAK/WinTAK provides ground users and pilots a meaningful, geospatial site picture and inter-operates with other situational awareness tools including SpyGlass, RaptorX, FalconView, and other legacy systems. Both support most of the standardized image/map formats. Its standalone capabilities include moving map functions independent of cellular/Wi-Fi network. Additionally, these mobile applications allow maps to be loaded during mission pre-planning or execution phase. It utilizes internal and external GPS sources

56. ATAK/WinTAK variations are currently utilized by many branches of federal, state, and local governments and partner nations.

57. Draper, one of the nation's leading technology developers for national security, will build on its support for the warfighter under a new contract to operate and maintain the Tactical Assault Kit, or TAK, a widely used communications system for the military. The company recently received a sole-source contract with the Defense Threat Reduction Agency (DTRA) of the U.S. Department of Defense.

58. The $415,000 contract calls for Draper to provide maintenance support, technical services, testing, evaluation and training for TAK. The TAK application supports the Nuclear Enterprise Contingency Operations Department's (NE-COs) various chemical, biological, radiological and nuclear (CBRN) detector systems.

59. Draper has developed software for every version of TAK since it was first developed by the Department of Defense. The software is available as ATAK for Android devices, WinTAK for Windows and WebTAK for the web. The company's long experience with the application and with warfighter systems overall were major reasons Draper will expand its role from research and development to operation and maintenance of the TAK platform, according to Brian Alligood, Draper's program manager for TAK. https://www.draper.com/news-releases/draper-tapped-us-department-defense-provide-services-and-support-tactical-assault-kit

60. Tactical Assault Kit (TAK) is a situational awareness solution designed for military and first responder personnel. On the original development team for ATAK for Android devices under the U.S. Air Force Research Laboratory, Draper contributed to initial design and core software. Draper also worked on WinTAK for Windows, and it developed WebTAK as a browser-based capability.

61. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into TAK, collect CBRN sensor data, display it on a map and livestream it across the TAK network to other users. CBRN plugins for ATAK, WinTAK and WebTAK are operational in the field.

62. Below, is an illustrative claim chart of how the HP ZBook PC directly infringes claim 5 of Golden's '287 patent, and claim 1 of Golden's '189 patent.

63. To satisfy the limitation for CBRN that is internal the HP ZBook PC is Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals. Intel Labs' Nabil Imam holds a Loihi neuro-morphic chip in his Santa Clara, California, neuro-morphic computing lab. (Walden Kirsch/Intel Corp)

64. To satisfy the limitation for CBRN that is external the HP ZBook PC is WinTAK. WinTAK was developed to provide a Windows-based application. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into WinTAK.